UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF: OF AN APPLE IPHONE 8, SERIAL# C8PVH0VVJC6C IN THE CUSTODY OF HSI MANCHESTER, NH	Case No. 21-mj-231-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ronald Morin, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), being duly sworn, do depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing a search of an Apple iPhone 8, Serial# C8PVH0VVJC6C (SUBJECT DEVICE), further described in Attachment A, for the things described in Attachment B—specifically, evidence, fruits, and instrumentalities of the foregoing criminal violations which relate to production, receipt, distribution and possession of child pornography, and sex trafficking of minors.

2. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), and have been so employed since May 2006. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation, child pornography, and human trafficking. I have received training in the area of child pornography and child exploitation, and as part of my

duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The statements in this affidavit are based on my own investigation of this matter as well as on information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. While I have included all material facts relevant to the requested search warrant, I have not set forth all of my knowledge about this matter.

5. I submit that the facts set forth in this affidavit establish probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, and 1591 have been committed and that there is probable cause to believe that fruits, evidence, and instrumentalities of the Specified Federal Offenses are likely to be found in the SUBJECT DEVICE, as set forth below.

SPECIFIED FEDERAL OFFENSES

6. Title 18, United States Code, Section 2251(a) makes it unlawful for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitting using any means or facility of interstate or foreign commerce, or if such visual depiction was produced or

transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. Title 18, United States Code, Section 2252(a)(2) makes it unlawful for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. Title 18, United States Code, Section 2252(a)(4)(B) prohibits any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

9. Title 18, United States Code, Section 1591(a)(1) makes it unlawful for any person to knowingly, in or affecting interstate or foreign commerce, recruit, entice, harbor, transport, provide, obtain, maintain, patronize, or solicit by any means a person, knowing or in reckless disregard of the fact that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act.

DEFINITIONS

10. The following definitions apply to this Affidavit and Attachment B:

a) "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b) "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

c) "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

d) "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

e) "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic

or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

PROBABLE CAUSE

11. On 08/06/2021, Alton Police Department (APD) Detective Adam Painchaud met with John Doe 1 (hereafter "JD1"/identity known by police). JDl, a male under the age of 18, arrived to APD to report having been solicited by his former boss for pictures and videos of himself masturbating in exchange for money. He additionally reported having been subjected to oral sex by his boss on several occasions, where his former boss gave him oral sex. JD1 identified the person to have given him oral sex and to whom he sent pictures and videos as JOHN MURRAY, the manager at the West Alton Marina (35 W Alton Marina Road, Alton, NH 03810) where JD1 worked at the time.

12. On 08/11/2021, a Child Advocacy Center (CAC) forensic interview of JDl was conducted. During the course of the interview, JDl disclosed that MURRAY had provided him cash, typically in the form of $100 bills in exchange for videos and pictures of JD1 masturbating, specifically "cum shots" (ejaculation videos). JD1 said MURRAY gave him specific instructions on how he wanted JDl to send the videos to him on Snapchat so the videos could be saved and viewed more than once (AGENT'S NOTE: MURRAY has Snapchat username "h20boss"). Through my training and experience, I am aware that Snapchat is a mobile application made by Snap Inc. and available through the iPhone App Store and Google Play that allows users to communicate and exchange text, photo, and video-based messages. JDl felt obligated to send the videos and did not want to disappoint MURRAY. MURRAY told JD l not to tell anyone about it and to keep it between them. JDl described that he had sent 15-20 videos of himself masturbating, as directed by MURRAY, in exchange for cash from MURRAY.

13. JD1 disclosed several occasions when MURRAY fondled his penis. JD1 said MURRAY would pull JDl's pants down and would play with his penis and testicles with his hands. JD1 described the first time it had occurred was in MURRAY'S office at the Marina. JD1 felt uncomfortable with the act. JD1 said he "felt frozen" and his entire body was tense, and his fists clinched at his sides. JDl wanted it to stop but did not want to upset MURRAY. JDl tried to continue working an administrative task as MURRAY sexually assaulted him. MURRAY then put JD1 's penis in his mouth. JD1 described just staring at a wall as MURRAY perform oral sex on him.

14. JD1 described another specific time when MURRAY brought him into a utility closet at the Marina and closed the door and turned off the lights and then pulled JD1 's shorts down. MURRAY then played with JD1's penis with his hands in an attempt to get him more erect. MURRAY then put JDl 's penis in his mouth and performed oral sex on him. JD1 said he felt like his feet were "pressing into the floor" as he was so tense.

15. On at least one occasion, MURRAY offered JDl $500 if JD1 would ejaculate in MURRAY'S mouth. JD1 did not accept this offer.

16. JDl described these fondling and oral assaults happened to him almost daily while working for MURRAY. JD1 said MURRAY gave him oral sex on the Marina property at least 10 times and up to 20 times and fondled his penis many more times than that. JD1 said he would try not to think about the acts as they were happening. All of the sex acts occurred on the Marina property.

17. JDl spoke of John Doe 2, 3, 4, and 5, (identities known by police) each male under the age of 18 at the time, and each employee of West Alton Marina under MURRAY's supervision at the time, as other people he knew had been sexually assaulted by MURRAY and

of whom MURRAY had solicited and received images and videos of them masturbating. JDl said these things were known by many of the employees around the Marina.

18. On 08/11/2021 a CAC forensic interview was conducted of JD2. When asked why he was in the interview JD2 said, "my boss has done some terrible things that is effecting everyone". JD2 went on to disclose he had sent explicit videos and pictures of himself to MURRAY in exchange for cash, on several occasions. JD2 described MURRAY asked him for the content and told him “These could keep coming" in reference to the $100 bills he was paid for the media content. MURRAY specified how he wanted JD2 to send him videos in a format that could be saved on Snapchat (AGENT’S NOTE: MURRAY has Snapchat username “h20boss”). JD2 talked about the first time MURRAY asked him for "nudes" and MURRAY gave him a $100 bill following sending him pictures and said, "nice cock". MURRAY specifically asked JD2 to send him videos of him "jerking off". JD2 said this happened once every week or two while working at the Marina for MURRAY.

19. APD Detective Painchaud examined JD2's phone and observed videos of JD2 masturbating and ejaculating that he had sent to MURRAY's phone via Snapchat.

20. JD2 identified JD3, JD4, and JD5 as others who had been victimized by MURRAY. JD2 was aware those individuals had performed sexual acts with MURRAY and sent MURRAY explicit content of themselves in the past. JD2 said he had been warned by JD4 prior to working for MURRAY about his behavior.

21. APD Detective Painchaud interviewed another witness (identity known by police) who spoke about a “jack shack” somewhere behind a bath house on the Marina property where MURRAY engaged in sexual acts. The witness stated that MURRAY had been caught filming an underage boy in the Marina bathhouse and the boy told his dad (a boat slip renter), who in

turn confronted MURRAY about it. The father filed a complaint with the Marina regarding this incident, and the owner of the Marina, Brian Fortier, was alerted.

22. JD2 spoke about doing work for MURRAY at the residence during his interview. JD2's mother knew that JD2 spent a significant amount of time with MURRAY at the residence and was concerned about that fact.

23. JD4, who worked for MURRAY at the Marina when he was under the age of 18, discussed the "naked" hot tub at the residence. JD4 had gone in the hot tub naked at the residence while working for MURRAY.

24. JD8 also spoke about the hot tub at the residence and said they (other kids) would often go in the hot tub without clothes on. JD8 said the hot tub was known by all to be a "no clothes" hot tub. JD8 said MURRAY had recently (this summer) taken a picture of the boys in the hot tub at the residence. During an interview on 8/17/2021, the mother of another JD (identity known by police), who was 15 years old when they worked for MURRAY at the Marina, told her "kids" were always over at the residence in the hot tub. Marcus Provost, an adult cousin of MURRAY who resides at the residence with MURRAY and Fortier, also spoke about the fact the hot tub was a "naked" hot tub and that it was MURRAY's "rule".

25. On 08/25/2021, a 16-year-old witness (identity known by police) who worked at the Marina for MURRAY disclosed that MURRAY had sent a picture out of all the boys naked in the hot tub at the residence. She observed the picture that MURRAY sent out.

26. On 08/12/2021, Belknap County Circuit Court Judge Michael H. Garner issued a State Search Warrant for MURRAY's Apple iPhone using telephone number [redacted] 2311, mobile phones, and other mobile communication devices. Based on the initial disclosures made by JD1 and JD2, the warrant authorized the seizure of responsive electronic data within a limited

timeframe—specifically, from June 2019 to present.

27. On 08/12/2021, APD Detective Painchaud went to MURRAY's residence at [redacted] Timber Ridge Road, Alton, NH (residence), with the state search warrant referenced in Paragraph 29, above. MURRAY relinquished an iPhone and iPad to Detective Painchaud pursuant to the warrant. Detective Painchaud asked MURRAY if he was aware of what the matter may be about. MURRAY went on to say he works with a lot of "kids" at the Marina. MURRAY described the kids as seasonal employees of whom he had approximately 20 annually. MURRAY surmised they say things and thought it may have something to do with one of them. During the course of the conversation, MURRAY named several of the kids in question. Two of the names MURRAY mentioned are John Does listed in this affidavit. Detective Painchaud asked MURRAY about an older iPhone that he previously used. [AGENT'S NOTE: During the course of the investigation, Detective Painchaud was advised that MURRAY was also known to have an older model iPhone or had used an older model iPhone in the past.] MURRAY stated that he didn't have the device and thought he "turned it in".

28. On 08/12/2021, APD Detective Painchaud arrested MURRAY on probable cause and charged him with two (2) counts of Aggravated Felonious Sexual Assault, two (2) counts of Felonious sexual assault, and three (3) counts of Manufacture of Child Sexual Abuse Images (CSAI), in violation of NH LAW. MURRAY refused bail and was subsequently transported to the Belknap County Jail. On 8/13/2021, at the bail hearing, Belknap Superior Court Judge James D. O'Neill III ruled that MURRAY was a danger to the community and ordered he be held in jail on preventative detention.

29. Examination of the contents of MURRAY's iPhone 12 Pro pursuant to a federal

search warrant is ongoing. However, preliminary findings on the device include the following:

- text messages MURRAY sent to another person wherein he described having "circle jerks" and oral sex with JDl and specifically mentioned all the "teen cum;"
- several videos and images appearing to meet the statutory definition of child pornography;
- distribution to at least two separate individuals of files that depict JD2 masturbating;
- masturbation videos and images of JD9 (MINOR 16yo/identity known by police), and distribution of these files to others via instant message.
- photographs taken outdoors at the residence that appear to depict nude, teenage boys posing together for photographs. At least one of the boys depicted in this series of photographs is identifiable as JD8. It is suspected, but not yet confirmed, that some of the other boys pictured are also JDs mentioned in this affidavit. [NOTE: These appear to be the "hot tub" photographs described above.]
- a text conversation in which MURRAY discusses engaging in sex acts with JD2. In this text conversation, MURRAY falsely refers to JD2 as being 18 years old.
- a text conversation in which MURRAY falsely refers to JD1 as being 18 years old.
- a deleted text conversation from the morning of August 6, 2021, wherein JD1 tells MURRAY he is quitting his job at the Marina and confronts MURRAY about the sexual assaults.
- "Ring" application installed on the device. Ring LLC is a home security and smart home company owned by Amazon. The investigation revealed that MURRAY has a Ring security camera installed outside his office at the Marina. It is unknown whether there are additional security cameras at the residence.

30. On 08/22/2021, APD Detective Painchaud received an email from Fortier who advised that he had two additional electronic devices that belong to MURRAY that he wanted to turn over to police. Detective Painchaud met with Fortier at the Marina the following day, and Fortier provided Detective Painchaud with MURRAY's devices, an iPhone 6S (IMEI 355424074978449) and an iPad (IMEI 351978065265581). Based on the nature of the investigation and allegations against MURRAY, Fortier stated that he was concerned that there may be child pornography on the devices.

31. Examination of the contents of MURRAY's iPhone 6S pursuant to a federal search warrant is ongoing. While looking at the "device information" for this iPhone in Cellebrite, HSI TFO Charles Pendlebury observed the following information which identified that this device belongs to John MURRAY. They are as follows:

a. The Apple ID associated with this device is Sledstud714 [redacted]. This email address is known to belong to John MURRAY and the numbers "714" are taken from MURRAY's birthday of [redacted] 1966.

b. The phone number associated with this phone is 603-520-2311 which is also known to belong to MURRAY.

32. While reviewing the phone on 09/02/2021, HSI TFO Pendlebury identified a communication thread between Brian Fortier and John MURRAY in "Native Messages". The participants for this chat are listed as (1) Brian Fortier [redacted] 3358; and (2) Jackson John (owner) Sledstud714 [redacted]. The start date of this communication is 08/30/2020 and the last activity date for this chat is 02/19/2021. In this chat there is a green text bubble with the name "Me" and a blue text bubble with the name "Brian Fortier". The green texts from the name

"me" refer to MURRAY's chats as being the owner of the device. The blue text bubbles are chats sent from Fortier. Most of this chat appears to be normal communication between partners, which Fortier and Murray are known to be. They discuss home life, what's for dinner, letting their dogs out, what to pick up at stores, work related conversation for their business at the West Alton Marina, and some sexual talk. HSI TFO Pendlebury noticed a conversation which occurred on 02/05/2021. The details are as follows:

> ME: [JD2][1] really wants to work (1120 UTC)
> BF (Brian Fortier): - Work what? (1122 UTC)
> BF: Dades cock (1123 UTC)
> ME: No helping at the marina (1136 UTC)
> BF: (two face emojis) one looks like a winking face the other is a devil emoji (1139 UTC)
> ME: Behave (1201 UTC)

33. On 09/07/2021, HSI TFO Pendlebury located more communication between Fortier and MURRAY referencing JD2. This communication occurred on 2/7/21 and is as follows:

> BF: How is [JD2's] cock? (1759 UTC)
> ME: Can you believe back in 1999 I had the balls to take those velocities out that's when I had confidence (1800 UTC). (AGENT NOTE: this is below Fortier's comment about [JD2's] cock but does not appear to be the response.)
> ME: Small (1800 UTC)
> BF: I saw it. How's it taste? (1800 UTC)
> ME: I know you saw it I'm not stupid
> ME: I don't know I'm too old and fat for him to get it up in front of me (1801 UTC)
> ME: I just like to tease me with it (1801 UTC) (AGENT NOTE: HSI TFO Pendlebury believes where MURRAY says "I" he means "He", as in JD2)
> ME: From all indicators I believe he falls around with his father as well as the dad of a friend of his as I told you (1801 UTC)

34. Since the initial disclosures made by JD1 and JD2, additional victims have been identified, some of whom are now adults who have not worked at the Marina in several years.

[1] The text message used JD2's name. I have replaced JD2's name with "JD2" throughout the chat wherever JD2's given name was used by MURRAY or Fortier.

Most of the alleged victims were recurring seasonal employees of the Marina who were between 15-17 years old at the time of the alleged criminal conduct. MURRAY has been employed at the marina for at least the past 10 years and was the direct supervisor of all of the alleged victims.

35. On 09/03/2021, District of New Hampshire United States Magistrate Judge Daniel J. Lynch authorized a Federal Search Warrant for the residence of MURRAY and Brian Fortier located at Timber Ridge Road, Alton, NH 03810, which included the search and seizure of mobile "smart" telephones.

36. On 09/09/2021 at approximately 0640 hours, HSI Special Agents, with the assistance of the New Hampshire State Police (NHSP), the Alton Police Department (APD), and members of the New Hampshire Internet Crimes Against Children (NH ICAC) executed the Federal Search Warrant at MURRAY/Fortier residence, Timber Ridge Road, Alton, NH.

37. HSI Special Agent (SA) Ronald Morin encountered Evan Mattson, DOB: 1998, a resident at Timber Ridge Road, Alton, NH, and an employee at West Alton Marina. Mattson advised SA Morin that Brian Fortier was currently "at the gym".

38. APD Detective Painchaud requested a uniformed APD Officer go to the gym to notify Fortier that law enforcement was at his residence executing a search warrant.

39. On 09/09/2021 at approximately 0725 hours Fortier arrived at his residence of Timber Ridge Road, Alton, NH. SA Morin identified himself and explained that law enforcement investigators were executing a Federal Search Warrant at his residence and at the business of West Alton Marina. SA Morin asked Fortier if he was the owner of West Alton Marina. Fortier responded that he was "part owner", along with his sisters Alyson and Deidre.

40. SA Morin asked Fortier for the telephone numbers of his sisters, Alyson and Deidre. Fortier removed his cellular telephone (SUBJECT DEVICE) from the front pocket of

his shorts. Fortier accessed the data on the SUBJECT DEVICE and provided investigators with the telephone numbers for his sisters, Deidre Tibbetts [redacted] 7705 and Allison Shea [redacted] 7610.

41. SA Morin asked Fortier for the SUBJECT DEVICE. Fortier handed SA Morin the SUBJECT DEVICE. SA Morin asked Fortier if he would share his passcode for the SUBJECT DEVICE. Fortier attempted to recall the numerical passcode but could not. Fortier asked SA Morin for the SUBJECT DEVICE back so he could manually enter the numerical code. SA Morin handed the SUBJECT DEVICE back to Fortier. Fortier tried several unsuccessful attempts to unlock the SUBJECT DEVICE. Fortier then used his finger (biometrics) and successfully unlocked the SUBJECT DEVICE. Fortier then handed the SUBJECT DEVICE to SA Morin. SA Morin placed the SUBJECT DEVICE in "airplane mode" to protect the integrity of its data. A few moments later, Fortier recalled the numerical passcode and stated "204862".

42. SA Morin advised Fortier that the Federal Search Warrant authorized the search and seizure of electronic devices on the premises ([redacted] Timber Ridge Road, Alton, NH), including the SUBJECT DEVICE. SA Morin further advised Fortier that since he initially was not on the premises, but has now returned onto the premises, SA Morin was detaining his phone and would apply for a separate Federal Search Warrant for the SUBJECT DEVICE. Though I believe seizure of the SUBJECT DEVICE was authorized by the existing warrant, I am seeking to obtain this warrant out of an abundance of caution.

43. A few minutes later, APD Detective Painchaud advised SA Morin that he received notice from Attorney William Christie of Shaheen & Gordon law firm advising investigators that Fortier is represented by counsel. Though Attorney Christie had apparently

tried to call APD Detective Painchaud and e-mailed APD Detective Painchaud before investigators spoke to Fortier, APD Detective Painchaud did not see the e-mail or the missed calls on his phone until after the SUBJECT DEVICE had been seized and investigators were already speaking to Fortier. Upon learning that he was represented, SA Morin advised Fortier that Investigators would not discuss the investigation further, as he is represented by an attorney.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

44. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT DEVICE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

45. I submit that if a computer or storage medium is found on the SUBJECT DEVICE, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

e. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

f. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can

also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

46. As set forth above, probable cause exists to believe that MURRAY has produced, distributed, received and/or possessed child pornography, and child pornography may be located on a variety of electronic devices and storage media owned and/or used by MURRAY. Based upon my knowledge and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides

and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification.

b. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

c. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

d. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

47. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the

warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

CONCLUSION

48. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 1591 may be located at the SUBJECT DEVICE. I therefore seek a warrant to search the SUBJECT DEVICE described in Attachment A and to seize the items described in Attachment B.

/s/ Ronald Morin
Special Agent Ronald Morin
Department of Homeland Security
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. P. 41 and affirmed under oath the contents of this affidavit and application.

Date: Sep 10, 2021

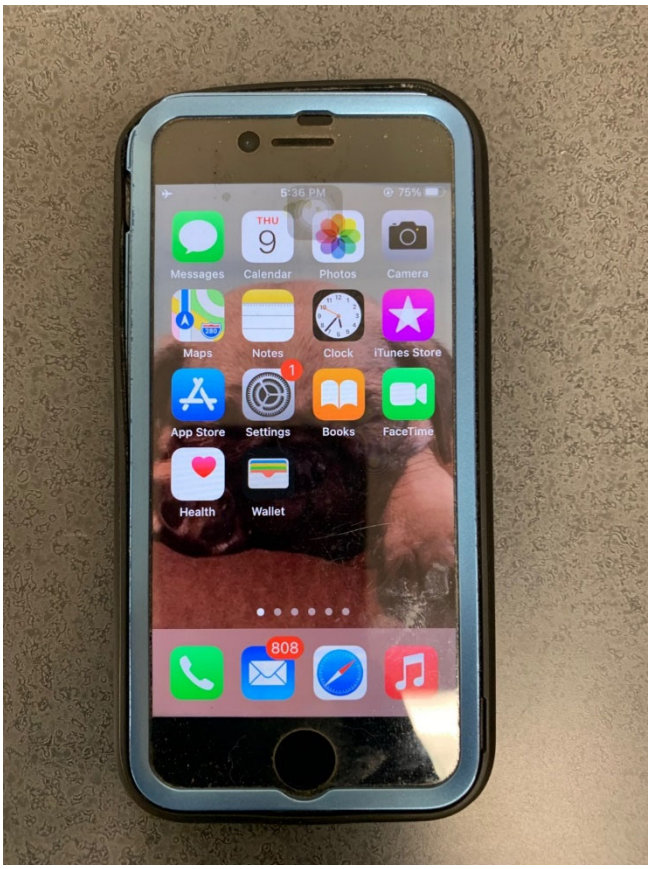
Time: 5:16 PM Sep 10, 2021

Andrea K. Johnstone
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

ATTACHMENT A

The device to be searched is an Apple iPhone 8, Serial# C8PVH0VVJC6C ("SUBJECT DEVICE"), now in custody of HSI Manchester, 275 Chestnut Street, Manchester, NH.



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252(a)(2), 2252(a)(4)(B), and 1591(a)(1):

1. All records relating to violations of 18 U.S.C. Sections 2251, 2252(a)(2), 2252(a)(4)(B), and 1591(a)(1) in any form wherever they may be stored or found on the SUBJECT DEVICE, including:

a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;

b. records or information pertaining to an interest in child pornography;

c. records or information pertaining to the production, possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

d. records or information of and relating to visual depictions that have been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256, including the record or information used to create the visual depiction;

e. photo-editing software and records or information relating to photo-editing software;

f. records or information relating to the ownership, possession, or use of electronic devices;

g. video surveillance data;

h. records or information pertaining to Snapchat;

i. records or information that contain any address, telephone number, computer screen name, user name, physical description, or other

information about any victim or other minor individual who is or may be a victim or intended victim of any of the offenses described herein;

j. any communications, in any form, that pertain to MURRAY or FORTIER's contacts with minors;

k. any files, records, notes, documentation, or communications regarding any complaints against MURRAY involving any minor;

l. records or information relating to the occupancy or ownership of the 104 Timber Ridge Road, Alton, New Hampshire, including, but not limited to, utility and telephone bills, mail envelopes, vehicle registrations, tax bills, and other correspondence.

2. Any computer or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including 18 U.S.C. Sections 2251, 2252(a)(2), 2252(a)(4)(B), and 1591(a)(1).

3. For any computer, computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

4. Any business and employee/personnel records of West Alton Marina that may be found on the SUBJECT DEVICE, in any form in which they may be kept, pertaining to MURRAY or pertaining to any minor that has been employed at the West Alton Marina for the past 10 years.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "COMPUTER" includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and

diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).